Pwned by the Owner

Zoz
Months!

Fuck!

ebay
craigslist
Fuck!
...time passes...
Dear Valued Customer:

Your account at DynDNS.com is due to expire in 5 days. You can prevent your account from expiring here:

https://www.dyndns.com/account/confirm/hawt24_t04jyhfMfY0DuKuw

Why is my account expiring?

Inactive accounts are deleted after 30 days. An account is inactive when:

* You do not log into the account within a 30-day period
* You do not update any Dynamic DNS hostnames within a 30-day period

Visiting a Dynamic DNS hostname *does not* count as activity.

How can I keep my account active?

If you wish to keep your account active without logging in or updating hostnames every 30 days, you can purchase a Dynamic DNS Pro upgrade:

http://www.dyndns.com/services/upgrades/

If you do not need your account or do not remember what it is for, you may simply allow it to expire and recreate the account later.

Thank you for choosing DynDNS.com!

Sincerely,
The DynDNS.com Team
Dynamic Network Services Inc.
<table>
<thead>
<tr>
<th>Hostname</th>
<th>Service</th>
<th>Details</th>
<th>Last Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>fear-and-loathing.cannytrophic.com</td>
<td>Host</td>
<td>72.193.81.105</td>
<td>May 7, 2010 7:01 PM</td>
</tr>
</tbody>
</table>

» Host Update Logs

» Bulk Update IP Address And Service Type

WTF!
% nslookup 72.193.81.105
Server: 127.0.0.1
Address: 127.0.0.1#53

Non-authoritative answer:
105.81.193.72.in-addr.arpa name = ip72-193-81-105.lv.lv.cox.net.

Authoritative answers can be found from:
81.193.72.in-addr.arpa nameserver = ns.cox.net.
81.193.72.in-addr.arpa nameserver = ns.east.cox.net.
81.193.72.in-addr.arpa nameserver = ns.west.cox.net.
ns.cox.net internet address = 68.1.16.107
ns.east.cox.net internet address = 68.1.16.108
ns.west.cox.net internet address = 68.111.106.68
% ping -t 60 fear-and-loathing.cannytrophic.com
PING fear-and-loathing.cannytrophic.com (72.193.81.105): 56 data bytes
64 bytes from 72.193.81.105: icmp_seq=0 ttl=50 time=587.550 ms
64 bytes from 72.193.81.105: icmp_seq=1 ttl=50 time=616.106 ms
64 bytes from 72.193.81.105: icmp_seq=2 ttl=50 time=579.045 ms
64 bytes from 72.193.81.105: icmp_seq=3 ttl=50 time=535.899 ms
64 bytes from 72.193.81.105: icmp_seq=4 ttl=50 time=611.475 ms
64 bytes from 72.193.81.105: icmp_seq=5 ttl=50 time=580.169 ms
64 bytes from 72.193.81.105: icmp_seq=6 ttl=50 time=624.006 ms
64 bytes from 72.193.81.105: icmp_seq=7 ttl=50 time=692.520 ms
64 bytes from 72.193.81.105: icmp_seq=8 ttl=50 time=606.340 ms
64 bytes from 72.193.81.105: icmp_seq=9 ttl=50 time=536.899 ms
64 bytes from 72.193.81.105: icmp_seq=10 ttl=50 time=605.183 ms
64 bytes from 72.193.81.105: icmp_seq=11 ttl=50 time=577.075 ms
64 bytes from 72.193.81.105: icmp_seq=12 ttl=50 time=704.004 ms
64 bytes from 72.193.81.105: icmp_seq=13 ttl=50 time=642.844 ms
64 bytes from 72.193.81.105: icmp_seq=14 ttl=50 time=580.136 ms
64 bytes from 72.193.81.105: icmp_seq=15 ttl=50 time=608.136 ms
--- fear-and-loathing.cannytrophic.com ping statistics ---
60 packets transmitted, 0 received, 100% packet loss, time 60998ms

% while (1)
while?
% ping -t 60 fear-and-loathing.cannytrophic.com
while?
% end

64 bytes from 72.193.81.105: icmp_seq=0 ttl=50 time=587.550 ms
64 bytes from 72.193.81.105: icmp_seq=1 ttl=50 time=616.106 ms
64 bytes from 72.193.81.105: icmp_seq=2 ttl=50 time=579.045 ms
64 bytes from 72.193.81.105: icmp_seq=3 ttl=50 time=535.899 ms
64 bytes from 72.193.81.105: icmp_seq=4 ttl=50 time=611.475 ms
64 bytes from 72.193.81.105: icmp_seq=5 ttl=50 time=580.169 ms
64 bytes from 72.193.81.105: icmp_seq=6 ttl=50 time=624.006 ms
64 bytes from 72.193.81.105: icmp_seq=7 ttl=50 time=692.520 ms
64 bytes from 72.193.81.105: icmp_seq=8 ttl=50 time=606.340 ms
64 bytes from 72.193.81.105: icmp_seq=9 ttl=50 time=536.899 ms
64 bytes from 72.193.81.105: icmp_seq=10 ttl=50 time=605.183 ms
64 bytes from 72.193.81.105: icmp_seq=11 ttl=50 time=577.075 ms
64 bytes from 72.193.81.105: icmp_seq=12 ttl=50 time=704.004 ms
64 bytes from 72.193.81.105: icmp_seq=13 ttl=50 time=642.844 ms
64 bytes from 72.193.81.105: icmp_seq=14 ttl=50 time=580.136 ms
64 bytes from 72.193.81.105: icmp_seq=15 ttl=50 time=608.136 ms
--- fear-and-loathing.cannytrophic.com ping statistics ---
60 packets transmitted, 0 received, 100% packet loss, time 60998ms

% ssh fear-and-loathing.cannytrophic.com
Password:
Welcome to Darwin!

fear-and-loathing.cannytrophic.com:~ %

Fuck yeah!
mrnguzmanmel@gmail.com
✓ Location: Las Vegas

✓ Name: Mel Guzman

✓ Photos:

✓ GMail account: mrguzmanmel@gmail.com

✓ Keylogger installed
LogKext Daemon starting up : Mon May 10 22:14:25 2010

<esc><esc><tab>>>>kljhghggbjj<down><down><up><up>??

>>>:KLBYYYYYBAL:&&&&BJ<cmd>BJHZUXUY<cmd>&S^&N<del>

AMBERVALLEYLANE LAS VEGAS<tab>nnnnnnnn<tab>
youtube.com
dont lea<del>irs.com
irs
<cmd>tmocospace.com
1flyricanpapi<tab>guzman85
mrguzmanmel@gmail.com
melvin<tab>guzman<tab> amv<del>ber
valleylane<del><del><del><del>ln<shift><tab> <del>MFG
FGUVUTYRTERWEW#W#QW$SW$#D$W$#E#$RR%T%^&Y&R
$&**YR*TYJ*BR&B&B&HJJJUJJUYBUBJNICKJRNC<del>ICK JR
<cmd>CV XZ
{}}{+}{}
<table>
<thead>
<tr>
<th>Name</th>
<th>Kind</th>
<th>Date Modified</th>
<th>Keychain</th>
</tr>
</thead>
<tbody>
<tr>
<td>account.mycricket.com</td>
<td>Internet password</td>
<td>Apr 20, 2010 7:41:03 AM</td>
<td>zoz</td>
</tr>
<tr>
<td>login.yahoo.com</td>
<td>Internet password</td>
<td>Apr 20, 2010 5:23:37 PM</td>
<td>zoz</td>
</tr>
<tr>
<td>my.screenname.aol.com</td>
<td>Internet password</td>
<td>Apr 20, 2010 5:22:01 PM</td>
<td>zoz</td>
</tr>
<tr>
<td>nicp.njjoblink.org</td>
<td>Internet password</td>
<td>Apr 11, 2010 8:59:27 AM</td>
<td>zoz</td>
</tr>
<tr>
<td>Safari Forms AutoFill</td>
<td>application password</td>
<td>May 3, 2009 10:56:47 AM</td>
<td>zoz</td>
</tr>
<tr>
<td><a href="http://www.blackplanet.com">www.blackplanet.com</a></td>
<td>Internet password</td>
<td>Apr 13, 2010 2:16:21 AM</td>
<td>zoz</td>
</tr>
<tr>
<td><a href="http://www.facebook.com">www.facebook.com</a></td>
<td>Internet password</td>
<td>Apr 13, 2010 7:52:49 AM</td>
<td>zoz</td>
</tr>
<tr>
<td><a href="http://www.google.com">www.google.com</a></td>
<td>Internet password</td>
<td>Apr 10, 2010 7:50:34 AM</td>
<td>zoz</td>
</tr>
<tr>
<td><a href="http://www.mocospace.com">www.mocospace.com</a></td>
<td>Internet password</td>
<td>Apr 27, 2010 11:07:34 PM</td>
<td>zoz</td>
</tr>
<tr>
<td><a href="http://www.myspace.com">www.myspace.com</a></td>
<td>Internet password</td>
<td>Apr 20, 2010 1:42:36 PM</td>
<td>zoz</td>
</tr>
</tbody>
</table>
Melvin,

Happy Birthday from Army.com!

Here's your Birthday Present! Get 25% off your next Army.com Store. Use the coupon code: HAPPYBDAY03 at checkout.

This coupon expires on April 7, 2010
mocospace.com: 1flyricanpapi / guzman85

gmail: mrguzmanmel@gmail.com / guzman85

PayPal: mrguzmanmel@gmail.com / guzman85

Facebook: timrican@yahoo.com / guzman85

Yahoo: timrican / guzman85

BlackPlanet.com: fricanpapi85 / guzman85

BlackCrush.com: fricanpapi / guzman85

yourfuckbook.com: fricanpapi / guzman85

planetsuzy.com: fricanpapi / guzman85

cect-forums.com: melguzman85 / guzman85

eBay: mguzman1985
Name: Melvin Guzman-Rosa

Address: Amber Valley Lane, Las Vegas, NV

Birthday: March 27, 1985
Hello melvin guzman-rosa,

You sent a payment of $10.99 USD to Game Time Zone (support@gametimezone.com)

It may take a few moments for this transaction to appear in your account.

Merchant
Game Time Zone
support@gametimezone.com

Instructions to merchant
You haven't entered any instructions.

Shipping address - confirmed
melvin guzman-rosa
8528 amber valley
las vegas, NV 89134
United States

Shipping details
The seller hasn't provided any shipping details yet.

<table>
<thead>
<tr>
<th>Description</th>
<th>Unit price</th>
<th>Qty</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Xbox 360 Live 1 Month Gold Card (Worldwide) Item# gzt89413</td>
<td>$10.99 USD</td>
<td>1</td>
<td>$10.99 USD</td>
</tr>
</tbody>
</table>

Subtotal | $10.99 USD |
Total    | $10.99 USD |

Payment | $10.99 USD |
Charge will appear on your credit card statement as "PAYPAL *GAMETIMEZONE"
Payment sent to support@gametimezone.com
Nevada EPPICard  the safe and secure way to access your payments!

Login to Your Account

If the image and identifier below match your profile image and identifier you can securely log into our site using your password. Not seeing your image or identifier? Don't sign on.

BALD EAGLE

User ID
MELVINGU
Password
Password
Reset Password?

Login  Cancel

Help?

Privacy Policy  Contact Us
Client Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>MELVIN GUZMAN-ROSA</td>
<td>9528 AMBER VALLEY LANE LAS VEGAS, NV 891340000</td>
</tr>
</tbody>
</table>

Client Cards and Balances

<table>
<thead>
<tr>
<th>Card Number</th>
<th>Status</th>
<th>Issue Date</th>
<th>Expire Date</th>
<th>Freeze Date</th>
<th>Cash Balance</th>
</tr>
</thead>
<tbody>
<tr>
<td>442728XXXXXX3077</td>
<td>REGISTERED</td>
<td>04/20/2010</td>
<td>04/30/2013</td>
<td></td>
<td>$2.92</td>
</tr>
</tbody>
</table>

Automated Deposit Notification

<table>
<thead>
<tr>
<th>Method of Contact</th>
<th>Email</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone</td>
<td><a href="mailto:timrican@yahoo.com">timrican@yahoo.com</a></td>
<td>7027885565</td>
</tr>
</tbody>
</table>
Melvn Guzman

The things you care about will now link to actual Pages
We matched your current profile info to related Pages.

View Page suggestions ▸

Basic Information

Sex: Male
Birthday: March 27, 1985
Hometown: lakewood ca, Los Angeles, CA
Siblings: alex guzman, xavier guzman
Relationship Status: Single
Interested In: Women
Looking For: Friendship
Contact Information

Email: timrican@yahoo.com
Mobile Number: 562-467-3357
Yahoo: lilprprettyboy
AIM: puertoricanqt352
College: cerritos '04
This message is from a Virgin Mobile user. Enjoy.

* n god i trust*
Compose a Note
You are about to send a note. Your note will be stored in your Sent Notes folder.

Subject: 

Message: (no HTML)
hey sweety how r u doing ma im devin nice to meet u... so how is ur day going ... i just moved back out here from florida then call before that here for training in mma fighting.. u look mad gorgeous and definetly sexy in them pics i would luv to earn ut time and get to no u if thats cool luv hit me back

0 : 10,000

Use signature

To help us fight spam. Type the two words.

35 dillon

Product of CAPTCHA | stop spam. read books
Compose a Note
You are about to send a note. Your note will be stored in your Sent Notes folder.

Subject: CRISTAL 702

Message: (no HTML)

hey sweetie how r u doing ma devin nice to meet u.. so how is ur day going ... i just moved back out here from florida then call before that here for training in mma fighting.. u look mad gorgeous and definitely sexy in them pics i would luv to earn ur time and get to no u if thats cool luv hit me back

0: 10,000

Use signature

To help us fight spam. Type the two words.

oil enrol

Product of CAPTCHA | stop spam. read books

Save Draft Send
hey how are you doing im currently looking for a room in the las vegas area im currently workin for ufc and im taking online course for criminal justice if you would like to more please ask me and ill be glad to answer any question im looking to in asap you can contact me at 5622613520
Lessons Learned

- Better security = non-recovery
- Perp could log in
- Network settings editable
- Recovered hardware & some data
- Potential vulns (against trained threat) were boons against low-tech threat
- ssh, VNC, IP tracking daemon
- Keychain vs keyloggers
- Note your serial #s for the cops
- Don’t fuck with a hacker’s machine